**IN THE CLAIMS:**

The text of all pending claims, (including withdrawn claims) is set forth below. Cancelled and not entered claims are indicated with claim number and status only. The claims as listed below show added text with underlining and deleted text with ~~strikethrough~~. The status of each claim is indicated with one of (original), (currently amended), (cancelled), (withdrawn), (new), (previously presented), or (not entered).

Please CANCEL claims 1-9, 16-21, 25, and 27 without prejudice:

1. (ORIGINAL) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

random number generator means for generating a random number;

q fixed values, where q is an integer; and

a first selector for selecting one of said q fixed values in response to the random number;

said XOR means XORing an input thereto with an XOR of a key with said selected fixed value.

2. (ORIGINAL) The encryption device according to claim 1, further comprising:

q sets of masked fixed tables; and

a second selector for selecting one of said q sets of fixed tables in response to the random number,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with the selected set of fixed tables.

3. (ORIGINAL) The encryption device according to claim 1, further comprising:

an encrypting unit comprising said first XOR means and said nonlinear transform means;

second XOR means for XORing an input to said encryption device with a fixed value selected in response to the random number; and

third XOR means for XORing an output from said encrypting unit with the fixed value selected in response to the random number.

4. (ORIGINAL) An encryption device comprising XOR means and nonlinear transform means, said encryption device further comprising:

random number generator means for generating a random number;

q sets of masked fixed tables, where q is an integer; and

a selector for selecting one of said q sets of fixed tables in response to the random number,

said nonlinear transform means nonlinearly transforming an input thereto in accordance with said selected set of fixed tables.

5. (ORIGINAL) The encryption device according to claim 4, further comprising

a plurality of encrypting rounds, wherein

each of said plurality of encrypting rounds comprises the XOR means, the fixed tables and the selector, for that round; and

the fixed tables for said plurality of respective encrypting rounds are identical.

6. (ORIGINAL) The encryption device according to claim 4, wherein

an equation, $(c_{0,j}$ XOR $c_{1,j}) \vee (c_{1,j}$ XOR $c_{2,j}) \vee ... \vee (c_{q-2,j}$ XOR $c_{q-2,j}) = (11111111)_2$, is satisfied, where a fixed table before masking is defined as S[x], and a j-th masked table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ (j = 0, 1, ... 15).

7. (ORIGINAL) The encryption device according to claim 4, wherein

the number of sets of tables is q = 2, and an equation, $c_{0,j}$ XOR $c_{1,j} = (10101010)_2$ or $(01010101)_2$, is satisfied, where a fixed table before masking is defined as S[x], and a j-th masked table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ (j = 0, 1, ... 15).

8. (ORIGINAL) The encryption device according to claim 4, wherein

an equation, $(d_{0,j}$ XOR $d_{1,j}) \vee (d_{1,j}$ XOR $d_{2,j}) \vee ... \vee (d_{q-2,j}$ XOR $d_{q-2,j}) = (11111111)_2$, is satisfied, where a fixed table before masking is defined as S[x], and a j-th masked table is defined as $S_j[x$ XOR $c_{i,j}]$ XOR $d_{i,j}$ (j = 0, 1, ... 15).

9. (ORIGINAL) The encryption device according to claim 4, said nonlinear transform means being Subbyte means;

said encryption device further comprising means for shifting an input, and means for mixedcolumning an input.

10. (CANCELLED)

11. (CANCELLED)

12. (CANCELLED)

13. (CANCELLED)

14. (CANCELLED)

15. (CANCELLED)

16. (ORIGINAL) An encryption device comprising random number generator means for generating a random number and a first plurality of encrypting rounds, wherein

each of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto, and XOR means for XORing a first input thereto with a second input thereto;

the second input to said XOR means is coupled to an output of said nonlinear transform means; and

said nonlinear transform means comprises:

q fixed values, where q is an integer;

a selector for selecting one of said q fixed values in response to the random number; and

further XOR means for XORing an input thereto with an XOR of a key with said selected fixed value.

17. (ORIGINAL) The encryption device according to claim 16, wherein

said nonlinear transform means further comprises therein a plurality of nonlinear transform means for nonlinearly transforming an input in accordance with a fixed table; and a selector for selecting one of said plurality of nonlinear transform means.

18. (ORIGINAL) The encryption device according to claim 17, wherein

the fixed tables of said respective nonlinear transform means in said respective encrypting rounds are identical.

19. (ORIGINAL) The encryption device according to claim 16, wherein

a mask is canceled over subsequent ones of said plurality of encrypting rounds.

20. (ORIGINAL) The encryption device according to claim 16, wherein masking is performed in each of a second plurality of encrypting rounds of said first plurality of encrypting rounds, said second plurality being smaller than said first plurality.

21. (ORIGINAL) An encryption device comprising a random number generator means for generating a random number, and a plurality of encrypting rounds, wherein

each of said plurality of encrypting rounds comprises nonlinear transform means for nonlinearly transforming an input thereto; and XOR means for XORing a first input thereto and a second input thereto;

the second input to said XOR means is connected to an output of said nonlinear transform means; and

said nonlinear transform means comprises therein nonlinear transform means for nonlinearly transforming an input thereto in accordance with a fixed table and in accordance with the random number.

22. (CANCELLED)

23. (CANCELLED)

24. (CANCELLED)

25. (ORIGINAL) A program stored on a storage medium for use in an encryption device, said program operable to effect the steps of:

selecting one of q fixed values, where q is an integer, in response to a random number;

XORing an input value with an XOR of a key with said selected fixed value;

selecting one set of q sets of masked fixed tables in response to the random number; and

nonlinearly transforming an input value in accordance with said selected set of fixed tables.

26. (CANCELLED)

27. (ORIGINAL) A program stored on a storage medium for use in an encryption device, said program operable to effect the steps of:

nonlinear transforming an input value to provide an output, and

XORing a first input value with said output as a second input value;

the nonlinear transforming step comprising the steps of:

selecting one of q fixed values in response to a random number, where q is an integer,

XORing an input value with an XOR of a key with said selected fixed value, and

nonlinear transforming an input value in accordance with a set of fixed tables associated with the random number.

28. (CANCELLED)